УДК 512.533.52, 519.161

С. В. Плещева, В. Вертеши

СЛОЖНОСТЬ ЗАДАЧИ ПРОВЕРКИ ТОЖДЕСТВ В ОДНОЙ КОНЕЧНОЙ 0-ПРОСТОЙ ПОЛУГРУППЕ*

1. Введение

В последнее время во всем мире активно развиваются исследования на стыке абстрактной алгебры и теории сложности вычислений. Взаимодействие этих дисциплин происходит во встречных направлениях. С одной стороны, алгебраические методы оказались весьма эффективными при анализе вычислительной сложности целого класса важных для теории и приложений комбинаторных задач, а именно ограниченных задач выполнимости (Constraint Satisfaction Problems), см., например, недавний обзор [1]. С другой стороны, многие алгебраические по своей сути задачи заинтересовали исследователей с точки зрения вычислительной сложности соответствующих алгоритмов (см., например, [2–5]).

В частности, одной из активно исследуемых задач является задача проверки тождеств в конечных алгебрах. Под *тождеством* понимается пара *термов* p и q (выражений, содержащих буквы некоторого алфавита, связанные между собой знаками операций данной алгебры). Тождество записывается посредством формального равенства $p \equiv q$. Некоторая алгебра *удовлетворяет* тождеству $p \equiv q$, или тождество $p \equiv q$ *выполнено* в этой алгебре, если при любой подстановке вместо букв тождества элементов алгебры значения выражений p и q будут равны. Во введенных терминах под задачей проверки тождеств понимается следующая комбинаторная задача распознавания, имеющая в качестве параметра заданную конечную алгебру $\mathcal{A}$:

УСЛОВИЕ: тождество $p \equiv q$.

ВОПРОС: Выполнено ли тождество $p \equiv q$ в алгебре $\mathcal{A}$?

Задачу проверки тождеств для данной алгебры $\mathcal{A}$ будем обозначать через ID-CHECK($\mathcal{A}$). Отметим, что в приведенной формулировке заданная конечная алгебра не включается в состав входного УСЛОВИЯ, а лишь играет роль предопределенного параметра. Это означает, что при анализе вычислительной сложности задачи ID-CHECK порядок алгебры считается заданной константой.

*Работа выполнена при поддержке РФФИ, проект № 05-01-00540.

В обзоре О. Харлампович и М. Сапира [6, проблема 2.4] анализ сложности задачи проверки тождеств упоминается среди наиболее интересных и естественно возникающих проблем. С тех пор в этой тематике наблюдаются значительные продвижения. Ниже мы приведем основные известные результаты.

Для обозначения классов вычислительной сложности используются стандартные обозначения P, NP, coNP (см. [7, 8] или раздел 2).

Прежде всего отметим, что для любой конечной алгебры $\mathcal{A}$ задача ID-CHECK($\mathcal{A}$) принадлежит классу сложности coNP, так как ее отрицание является задачей с полиномиальной проверкой, т. е. принадлежит классу NP.

Для ассоциативных колец в [9] получен критерий coNP-полноты данной задачи: она решается за полиномиальное время, если кольцо нильпотентно, и является coNP-полной в противном случае.

Для групп задача проверки тождеств исследована только частично, однако и здесь имеются существенные продвижения: в [10] была доказана coNP-полнота этой задачи для неразрешимых групп; Лоуренсом и Баррисом [11] была доказана полиномиальная разрешимость задачи ID-CHECK для нильпотентных и диэдральных групп.

Для полугрупп исследования начались с построения М. В. Волковым и В. Ю. Поповым [12] примера полугруппы порядка $\leq 2^{1700}$, для которой задача ID-CHECK является coNP-полной. Позднее были построены примеры полугрупп гораздо меньшего порядка. Так, А. Кисилевич [13] указал полугруппу порядка $< 2^{16}$ с coNP-полной задачей проверки тождеств; в этой же работе был приведен полиномиальный алгоритм, решающий задачу проверки тождеств для коммутативных полугрупп. Примерно в то же время В. Вертеши и Ч. Сабо [14] доказали coNP-полноту задач ID-CHECK($M_2(Z_2)$) и ID-CHECK($M_2(Z_3)$) для мультипликативных полугрупп матриц размера 2×2 и построили 13-элементную подполугруппу полугруппы $M_2(Z_3)$, для которой задача проверки тождеств остается coNP-полной. Результат О. Климы [15], независимо полученный также С. Сайфом [16], о coNP-полноте задачи ID-CHECK для 6-элементного моноида Брандта B_2^1 дает, вероятно, минимальный по числу элементов пример полугруппы, для которой задача проверки тождеств является сложной с вычислительной точки зрения.

В данной работе мы исследуем вычислительную сложность задачи ID-CHECK в одной 19-элементной 0-простой полугруппе, которую в дальнейшем будем обозначать через $\mathcal{M}$. Нами доказана coNP-полнота задачи ID-CHECK($\mathcal{M}$).

Необходимые предварительные сведения, касающиеся теории конечных 0-простых полугрупп, приведены в разделе 2. Описание самой полугруппы $\mathcal{M}$ и ее свойства приведены в разделе 3.

Для краткости условимся называть алгебру *легкой*, если задача проверки тождеств в ней решается за полиномиальное время. В противном случае алгебру будем называть *сложной*.

Интерес к рассматриваемой нами полугруппе $\mathcal{M}$ обусловлен несколькими обстоятельствами. Прежде всего, конечные 0-простые полугруппы играют важную роль в общей теории конечных полугрупп и возникают в качестве главных факторов в строении произвольной конечной полугруппы. Во-вторых, анализ существующих примеров и известных результатов привел нас к выводу, что $\mathcal{M}$ является минимальной по числу элементов 0-простой полугруппой, в которой задача проверки тождеств могла оказаться сложной (см. раздел 4). В-третьих, данная полугруппа дает пример сложной некомбинаторной рисовской полугруппы матричного типа, чья структурная группа легка, в противовес легкости всех комбинаторных рисовских полугрупп, подробно разобранных в недавней работе [17]. Тем самым мы дополнительно пролили свет на проблему, отмеченную там же (см. проблему 1), о сложности задачи проверки тождеств в некомбинаторных рисовских полугруппах.

Для доказательства coNP-полноты задачи ID-CHECK($\mathcal{M}$) мы используем специально построенные графовые конструкции, которые описаны в разделе 5. Разделы 7 и 8 посвящены сведению некоторой промежуточной графовой задачи, названной нами двудольной задачей о четных гомоморфизмах (которую будем обозначать через B-EVEN-HOM), к интересующей нас задаче ID-CHECK($\mathcal{M}$). В разделе 9 мы доказываем coNP-полноту сразу двух графовых задач для графа шестиугольника: задачи B-EVEN-HOM и задачи EVEN-HOM, полученной из B-EVEN-HOM отказом от двудольности. Мы доказали coNP-полноту задачи EVEN-HOM, сведя к ней отрицание NP-полной задачи RET(Hex) о ретракции графов (см. [18,19] или раздел 2) на граф шестиугольника Hex. Далее мы сводим задачу EVEN-HOM к задаче B-EVEN-HOM. Произведенные свед́ения можно выразить следующей цепочкой, используя общепринятое обозначение $A \geq_p B$ в значении «задача B полиномиально сводится к задаче A»:

$$\text{ID-CHECK}(\mathcal{M}) \geq_p \text{B-EVEN-HOM}(Hex) \geq_p \\ \geq_p \text{EVEN-HOM}(Hex) \geq_p \text{RET}(Hex).$$

Также в работе был описан полиномиальный от числа вершин входного графа алгоритм, строящий по данному двудольному графу граф с равными степенями соответствующих вершин в долях, используя всего две операции: перестановку вершин в долях и приписывание существующим ребрам дополнительной кратности.

В заключение отметим, что, к сожалению, исчерпывающей сводимости рассмотрения сложности задачи ID-CHECK для конечных полугрупп к их главным факторам, 0-простым полугруппам, не существует. Этот вывод можно сделать на основании того, что существуют такие полугруппы, у которых все главные факторы имеют полиномиально разрешимую задачу проверки тождеств, но сама полугруппа тем не менее сложна (см. [3]).

Авторы выражают искреннюю благодарность проф. М. В. Волкову за постановку задачи и постоянное внимание к работе, а также А. А. Булатову за ряд ценных замечаний и полезное обсуждение результатов данной статьи.

2. Предварительные сведения

Мы предполагаем знакомство с основными определениями и результатами теории конечных 0-простых полугрупп (см. [20]) и теории вычислительной сложности (см. [7,8]). Тем не менее в этом разделе мы напомним некоторые из них, а также приведем необходимый нам результат из теории сложности графовых задач. Читатель, хорошо владеющий данной тематикой, может сразу перейти к разделу 3.

2.1. Конечные 0-простые полугруппы

Полугруппа называется *простой*, если она не содержит собственных двусторонних идеалов. Полугруппа S с нулем 0 называется *0-простой*, если (i) $S^2 \neq 0$ и (ii) 0 есть единственный собственный двусторонний идеал из S.

Опишем конструкцию рисовских полугрупп матричного типа над группами с нулем. Пусть G – группа и $G^0 = G \cup 0$ – группа с нулем, полученная из G присоединением нуля 0. Пусть P – произвольная, но фиксированная матрица над G^0. Через Λ и I обозначим множества, индексирующие соответственно строки и столбцы матрицы P. Через $p_{\lambda i}$ обозначим элемент матрицы P, стоящий на пересечении строки с номером $\lambda \in \Lambda$ и столбца с номером $i \in I$. Рассмотрим множество S, состоящее из символа 0 и всех троек вида (i, g, λ), где $g \in G$, $i \in I, \lambda \in \Lambda$. Зададим умножение на элементах множества S по следующим правилам:

$$a \cdot 0 = 0 \cdot a = 0 \quad \text{для всех} \quad a \in S,$$

$$(i, g, \lambda) \cdot (j, h, \mu) = \begin{cases} (i, g \cdot p_{\lambda j} \cdot h, \mu), & \text{если } p_{\lambda j} \neq 0; \\ 0, & \text{если } p_{\lambda j} = 0. \end{cases}$$

Легко проверить, что заданное таким образом умножение ассоциативно, а значит, S становится полугруппой. Она называется *рисовской полугруппой матричного типа с сэндвич-матрицей P над группой с нулем G^0* и обозначается через $\mathcal{M}^0(G; I, \Lambda; P)$. Группа G называется *структурной группой* полугруппы $\mathcal{M}^0$. Следующее классическое утверждение связывает понятие 0-простоты для рисовской полугруппы со строением ее сэндвич-матрицы.

Предложение 2.1. *Рисовская полугруппа матричного типа является 0-простой тогда и только тогда, когда ее сэндвич-матрица содержит по крайней мере один ненулевой элемент в каждой строке и в каждом столбце.*

Такие матрицы, упомянутые в предложении, называются *регулярными.*

Также отметим, что в представлении данной конечной 0-простой полугруппы как регулярной рисовской полугруппы матричного типа ее сэндвич-матрицу можно изменять, не меняя при этом саму полугруппу (см. [20, гл. 3, § 3.2]). При этом используются следующие операции над матрицами: перестановка строк и столбцов, умножение строки слева или столбца справа на любой элемент структурной группы. Тем самым мы можем, например, так *нормализовать* матрицу, что каждый элемент в данной строке и данном столбце будет равен либо 0, либо единице структурной группы.

Иногда для сокращения записи вместо обозначения (i, g, λ) элемента рисовской полугруппы мы будем писать $\langle i, \lambda\rangle$, если нам не принципиален средний (групповой) элемент тройки. В следующей лемме перечислены некоторые свойства рисовских полугрупп. Все они являются непосредственными следствиями из определения закона умножения.

Лемма 2.1. *Пусть S – рисовская полугруппа матричного типа. Пусть дана последовательность $x_1, x_2, \ldots x_n \in S$, тогда:*

(1) $x_1 \cdot x_2 \cdot \ldots \cdot x_n = 0$ *тогда и только тогда, когда существует такой индекс* $k \in \{2, 3, \ldots n\}$, *что* $x_{k-1} \cdot x_k = 0$;

(2) *если* $x_1 \cdot x_2 \cdot \ldots \cdot x_n \neq 0$, *то* $x_1 \cdot x_2 \cdot \ldots \cdot x_n = \langle i_1, \lambda_n\rangle$, *где* $x_1 = \langle i_1, \lambda_1\rangle$, $x_n = \langle i_n, \lambda_n\rangle$.

Дадим определение фактор-полугруппы Риса. Пусть I – идеал полугруппы S. Определим отношение ρ на S, полагая $a\rho b$ $(a, b \in S)$ тогда и только тогда, когда либо $a = b$, либо a и b принадлежат I. Отношение ρ называется *конгруэнцией Риса по модулю I*. Классами эквивалентности полугруппы S по модулю ρ являются само I и каждое одноэлементное множество $\{a\}$, где $a \in S \setminus I$. Вместо S/ρ пишется S/I и называется *факторполугруппой Риса полугруппы S по модулю I*. Можно представлять себе S/I как результат сжатия I в один элемент (нуль), в то время как элементы из $S \setminus I$ не затрагиваются.

Также нам понадобится факторизация по отношению Грина $\mathcal{H}$. Для произвольной полугруппы $S = \mathcal{M}^0(G; I, \Lambda; P)$ подполугруппу $S/\mathcal{H}$ можно мыслить как объединение нуля и всех пар вида (i, λ), где $i \in I, \lambda \in \Lambda$, с сэндвич-умножением посредством матрицы P', полученной из P заменой всех ее ненулевых элементов на 1. Таким образом, $S/\mathcal{H} = \mathcal{M}^0(\{1\}; I, \Lambda; P')$ – рисовская полугруппа матричного типа над единичной группой, с 0–1 сэндвич-матрицей (такие полугруппы называют еще *комбинаторными*).

2.2. Классы вычислительной сложности

В теории вычислительной сложности под задачами подразумевают так называемые массовые задачи, задаваемые своими УСЛОВИЕМ и ВОПРОСОМ и объединяющие в себе множество конкретных задач. Каждая конкретизация подобной массовой задачи получается фиксированием УСЛОВИЯ.

Задача принадлежит классу P, если она решается за полиномиальное от размера УСЛОВИЯ время на *детерминированной машине Тьюринга* (см. [7, 8]). С практической точки зрения именно такие задачи можно назвать «легкими» по временным затратам. Задача принадлежит классу NP, если она решается за полиномиальное время на *недетерминированной машине Тьюринга.* Если угадав каким-то образом ответ задачи, мы можем за полиномиальное время на детерминированной машине Тьюринга этот ответ проверить, то задача называется *задачей с полиномиальной проверкой.* Все задачи с полиномиальной проверкой очевидно принадлежат классу NP. Задача принадлежит классу coNP, если ее отрицание принадлежит классу NP.

Задача A *полиномиально сводится* к задаче B, если существует полиномиальный алгоритм f, который по любой конкретизации a задачи A строит конкретизацию $f(a)$ задачи B так, что ответ на a положителен тогда и только тогда, когда ответ на $f(a)$ также положителен.

Задача называется NP [coNP]-*полной*, если она принадлежит классу NP [coNP] и к ней полиномиально сводится любая задача из класса NP [coNP].

2.3. Задачи на графах

Пусть H – граф. Через $V(H)$ и $E(H)$ обозначим соответственно множества его вершин и ребер. Под *гомоморфизмом* f графа G в граф H понимается вершинное отображение $f\colon V(G) \to V(H)$, сохраняющее ребра (т. е. для каждого ребра $(u, v) \in E(G)$ выполнено $(f(u), f(v)) \in E(H)$).

Подграф H графа G называется *ретрактом*, если существует такой гомоморфизм $f\colon G \to H$, что для любой вершины $v \in V(H)$ выполняется $f(v) = v$. Гомоморфизм f при этом называется *ретракцией* графа G на подграф H. Задачей ретракции $\mathrm{RET}(H)$ для заданного графа H называется следующая комбинаторная задача распознавания:

УСЛОВИЕ: граф G, имеющий в качестве подграфа граф H', изоморфный графу H.

ВОПРОС: Существует ли ретракция графа G на подграф H'?

Теорема 2.1 ([18, 19]). *Для любого цикла длины* ≥ 6 *задача ретракции* NP-*полна.*

Предложение 2.2. *Пусть C_n – цикл длины n. Ограничение задачи* $\mathrm{RET}(C_n)$ *на связные графы не умаляет ее сложности.*

Доказательство. Для доказательства необходимо свести общую задачу $\mathrm{RET}(C_n)$ к ее ограничению на связные графы. Для этого по каждому входному графу G построим такой связный граф G_1, что для графа G существует ретракция на цикл C_n тогда и только тогда, когда существует ретракция графа G_1 на цикл C_n. Мы будем пользоваться обозначением C_n, предполагая под этим изоморфную копию цикла длины n в рассматриваемом графе.

Предположим, что граф G не связен. Выберем его компоненту связности, в которой находится цикл C_n. Все остальные компоненты заиндексируем числами $i = 1, \ldots, m$ и в каждой такой компоненте K_i выберем по одной произвольной вершине v_i. Соединим каждую вершину v_i $(i = 1, \ldots, m)$ с произвольной вершиной цикла C_n, скажем w. В итоге получим связный граф, который обозначим через G_1. Необходимость существования ретракции при таком построении очевидна.

Докажем достаточность. Пусть $\varphi \colon G \to C_n$ – ретракция графа G на цикл C_n. Применим φ как вершинное отображение к графу G_1. Если при этом φ останется гомоморфизмом, то все доказано. Пусть φ не является гомоморфизмом графа G_1. Это означает, что какое-то ребро вида (v_i, w) перешло на несуществующее ребро цикла C_n, т. е. вершина $\varphi(v_i)$ не смежна с вершиной w в цикле. Так как $\varphi(K_i)$ – это некоторый путь в цикле C_n, то в силу поворотной симметрии C_n можно так дополнить $\varphi_{|K_i}$, что вершина v_i перейдет в вершину, смежную с w. Таким образом, несколько «подкрутив» отображение φ на каждой компоненте K_i, мы получим ретракцию графа G_1 на цикл C_n.

3. Описание полугруппы $\mathcal{M}$

Рассмотрим 2-элементную группу $\mathbb{C}_2 = \{a, e\}$, где e – это единица и $a^2 = e$. Пусть дана матрица

$$P = \begin{pmatrix} 0 & e & e \\ a & 0 & e \\ e & e & 0 \end{pmatrix}.$$

Исследуемая нами в данной работе полугруппа $\mathcal{M}$ – это рисовская полугруппа матричного типа $\mathcal{M}^0(\mathbb{C}_2; I, \Lambda; P)$ с сэндвич-матрицей P со структурной группой $\mathbb{C}_2$.

В следующей лемме перечислены некоторые свойства полугруппы $\mathcal{M}$. Все они являются непосредственными следствиями из определения закона умножения в $\mathcal{M}$. Напомним, что элемент x некоторой полугруппы называется *идемпотентом*, если выполняется равенство $x^2 = x$.

Лемма 3.1. *Пусть даны $x_1, x_2, \ldots x_n \in \mathcal{M}$, где $x_j = (i_j, g_j, \lambda_j)$. Тогда произведение $x_1 \cdot x_2 \cdot \ldots \cdot x_n$, если оно не нулевое, равно тройке $(i_1, a^k a^\ell, \lambda_n)$, где k – количество групповых элементов a среди g_j, ℓ – количество пар $\langle 2, 1\rangle$ среди всех пар $\langle \lambda_j, i_{j+1}\rangle$.*

4. Минимальность $\mathcal{M}$ среди «сложных» 0-простых полугрупп

Как и прежде, для краткости условимся называть алгебру *легкой*, если задача проверки тождеств в ней решается за полиномиальное время. В противном случае алгебру будем называть *сложной*.

Известно, что если структурная группа рисовской полугруппы матричного типа сложна, то и сама полугруппа сложна [17, предложение 5.1]. Таким образом, интерес представляют рисовские полугруппы с легкой структурной группой. Кроме этого, в силу предложения 2.1, сэндвич-матрицы рассматриваемых полугрупп должны быть регулярными. Сэндвич-матрицы, не содержащие элементов, отличных от нуля и единицы, будем называть 0–1 сэндвич-матрицами.

Порядок рисовской полугруппы матричного типа определяется порядком структурной группы и размером сэндвич-матрицы. Для обоснования минимальности выбранной нами полугруппы $\mathcal{M}$ среди всех сложных 0-простых рисовских полугрупп с простой структурной группой ниже мы последовательно рассмотрим всевозможные случаи размеров сэндвич-матриц и строения структурных групп. При этом мы будем использовать нормализацию сэндвич-матриц (см. раздел 2).

Следующий необходимый нам результат уже довольно давно известен и приведен, например, в обзоре [21, § 20] даже в более сильной форме. Однако для полноты картины, а также в силу легкости доказательства в конкретном случае, мы докажем его здесь.

Лемма 4.1. *Пусть $S = \mathcal{M}(G; I, \Lambda; P)$ – рисовская полугруппа матричного типа с 0–1 сэндвич-матрицей. Тогда тождество выполнено в полугруппе S тогда и только тогда, когда оно выполнено в структурной группе G и в комбинаторной рисовской полугруппе $\overline{S} = \mathcal{M}(\{1\}; I, \Lambda; P)$.*

Доказательство. Необходимость очевидна, так как G и $\overline{S}$ являются подполугруппами в S.

Докажем достаточность. Пусть дано тождество $x_1 \ldots x_n \equiv y_1 \ldots y_m$. Прежде всего заметим, что любое означивание слова в полугруппе S можно легко превратить в означивание в полугруппе $\overline{S}$, если вместо элемента (i, g, λ) написать (i, λ). Тогда по пункту (1) леммы 2.1 слово обращается в нуль при означивании в полугруппе S в том и только в том случае, когда оно обращается в нуль в полугруппе $\overline{S}$. Поскольку тождество выполнено в полугруппе $\overline{S}$, то слова этого тождества одновременно обращаются в нуль в $\overline{S}$ [17, лемма 4.2, предложение 4.10], а значит, и в полугруппе S.

Если же при означивании тождества в полугруппе S слова не обращаются в нуль, то результат означивания можно записать в виде $(i_1, g_1g_2 \dots g_n, \lambda_n) \equiv \equiv (j_1, h_1h_2 \dots h_m, \mu_m)$. Из выполнения данного тождества в полугруппе $\overline{S}$, по лемме 2.1(2), следует равенство $(i_1, \lambda_n) = (j_1, \mu_m)$. При этом выражение $g_1g_2 \dots g_n = h_1h_2 \dots h_m$ есть не что иное, как результат означивания исходного тождества в группе G, и, значит, обращается в верное равенство. Из всего сказанного следует, что данное тождество выполнено в полугруппе S.

Про комбинаторные рисовские полугруппы известно, что задача проверки тождеств в них легкая [17, раздел 4]. Следовательно, по лемме 4.1 получаем

Следствие 4.1. *Если структурная группа рисовской полугруппы матричного типа с 0–1 сэндвич-матрицей имеет полиномиально разрешимую задачу проверки тождеств, то полиномиально разрешима и задача проверки тождеств в самой полугруппе.*

Этим следствием мы будем неоднократно пользоваться при дальнейшем разборе случаев.

Случай 1. Если матрица имеет размеры 1×1, то умножением на обратный элемент всегда можно ее нормализовать к единичной. В таком случае несложно заметить, что данная рисовская полугруппа изоморфна своей структурной группе, а значит, по предположению, легка.

Случай 2. Если сэндвич-матрица имеет размеры 2×1, то умножением ее строк на обратные элементы мы можем любую такую матрицу нормализовать к виду $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Такие рисовские полугруппы, при условии легкости структурной группы, легкие по следствию 4.1.

Случай 3. Пусть сэндвич-матрица имеет размеры 2×2. Заметим, что в силу регулярности такая матрица не может содержать более двух нулей.

Подслучай 3.1. Пусть она совсем не содержит нулей. Тогда любую матрицу вида $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ можно нормализовать к виду $\begin{pmatrix} 1 & 1 \\ 1 & c^{-1}db^{-1}a \end{pmatrix}$. В случае матрицы, состоящей полностью из единиц, мы снова можем сослаться на следствие 4.1 для обоснования легкости соответствующей полугруппы. В случае матрицы вида $\begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix}$ полиномиальная разрешимость задачи проверки тождеств следует из [22, 23].

Подслучай 3.2. Пусть матрица содержит один или два нуля. Любую матрицу вида $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$ можно нормализовать к виду $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$; любую матрицу вида $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ можно нормализовать к виду $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Поэтому имеем рисовские полугруппы над легкой (в данном случае даже абелевой) структурной группой с 0–1 сэндвич-матрицей; такие полугруппы легкие по следствию 4.1. Отметим, что в случае 2×2 сэндвич-матрицы для получения рисовской полугруппы, содержащей менее 19 элементов, структурная группа должна содержать не более 4 элементов. Все такие группы, очевидно, абелевы.

Случай 4. Пусть сэндвич-матрица имеет размер 2×3. В этом случае для получения рисовской полугруппы, содержащей менее 19 элементов, структурная группа должна содержать не более 3 элементов. Следовательно, мы имеем три случая для структурных групп: единичная, циклическая второго порядка, циклическая третьего порядка. В случае единичной группы задача проверки тождеств полиномиально разрешима по следствию 4.1.

Подслучай 4.1. Пусть рисовская полугруппа имеет в качестве структурной двухэлементную группу $\mathbb{C}_2 = \{a, 1\}$. В силу регулярности сэндвич-матрица размера 2×3 не может содержать более трех нулей.

Подслучай 4.1.1. Если нулей нет, то любая матрица легко нормализуется или к виду $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, или к виду $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & a \end{pmatrix}$. В первом случае задача проверки тождеств имеет полиномиальное решение по следствию 4.1. Во втором случае такая рисовская полугруппа удовлетворяет в точности тем же тождествам, что и полугруппа $\mathcal{C}_2$ над группой $\mathbb{C}_2$ с сэндвич-матрицей $\begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix}$. Последняя полугруппа легкая. Оба результата можно найти в [22, 23].

Подслучай 4.1.2. Если есть один нуль, то любую матрицу можно нормализовать или к виду $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, или к виду $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & a \end{pmatrix}$. В первом случае мы имеем рисовскую матричную полугруппу над абелевой группой с 0–1 сэндвич-матрицей. Такая полугруппа легкая. Второй случай гораздо менее тривиален и заслуживает подробного разбора.

Обозначим через $\mathcal{S}$ рисовскую полугруппу матричного типа над группой $\mathbb{C}_2$ с сэндвич-матрицей $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & a \end{pmatrix}$. Через $\mathcal{C}_2$, как и выше, обозначим рисовскую полугруппу над группой $\mathbb{C}_2$ с сэндвич-матрицей $\begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix}$. Через $\mathcal{A}_2$ обозначим рисовскую полугруппу матричного типа над единичной группой с сэндвич-матрицей $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Полугруппы $\mathcal{C}_2$ и $\mathcal{A}_2$ легкие. Легкость полугруппы $\mathcal{S}$ получается в качестве непосредственного следствия из следующего предложения.

Предложение 4.1. *Тождество выполнено в полугруппе $\mathcal{S}$ тогда и только тогда, когда оно одновременно выполнено в $\mathcal{C}_2$ и в $\mathcal{A}_2$.*

Доказательство. Несложно проверить, что любой подматрице исходной сэндвич-матрицы рисовской полугруппы соответствует рисовская подполугруппа матричного типа. Подобным образом внутри полугруппы $\mathcal{S}$ можно найти подполугруппы $\mathcal{C}_2$ и $\mathcal{A}_2$. Следовательно, необходимость доказываемого предложения очевидна.

Для доказательства достаточности нам необходима следующая лемма, установленная в [24].

Лемма 4.2. *Пусть S – рисовская полугруппа матричного типа над группой G с сэндвич-матрицей P, а T – рисовская полугруппа матричного типа над группой H с сэндвич-матрицей Q. Рассмотрим в их прямом произведении $S \times T$ идеал I, состоящий из всех пар, в которых по крайней мере одна компонента равна 0. Тогда факторполугруппа $S \times T/I$ (ее называют 0-прямым произведением S и T) изоморфна рисовской полугруппе матричного типа над группой $G \times H$ с сэндвич-матрицей $P \otimes Q$ (тензорное или, в другой терминологии, кронекерово произведение матриц P и Q).*

Несложно заметить, что 0-прямое произведение удовлетворяет всем тем тождествам, которые выполнены одновременно в исходных полугруппах. Если применить лемму к полугруппам $\mathcal{C}_2$ и $\mathcal{A}_2$, то получим, что полугруппа над группой $\mathbb{C}_2 = \{a, 1\}$ с сэндвич-матрицей

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & 1 & a \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & a \end{pmatrix}$$

является 0-прямым произведением полугрупп $\mathcal{A}_2$ и $\mathcal{C}_2$, а следовательно, удовлетворяет всем тождествам, которые выполнены одновременно в полугруппах $\mathcal{A}_2$ и $\mathcal{C}_2$. Однако полугруппа $\mathcal{S}$ является подполугруппой в рассмотренном 0-прямом произведении, так как сэндвич-матрица полугруппы $\mathcal{S}$ получается пересечением трех последних столбцов с первой и последней строками сэндвич-матрицы 0-прямого произведения. Значит, полугруппа $\mathcal{S}$ также удовлетворяет всем тождествам, которые выполнены одновременно в полугруппах $\mathcal{A}_2$ и $\mathcal{C}_2$, что и требовалось доказать.

Подслучай 4.1.3. Если матрица содержит два или три нуля, то ее легко можно нормализовать к 0–1 матрице, и, значит, по следствию 4.1 вновь получаем легкость таких рисовских полугрупп.

Подслучай 4.2. Пусть рисовская полугруппа с сэндвич-матрицей размера 2×3 имеет в качестве структурной трехэлементную группу $\mathbb{C}_3 = \{1, a, b\}$. Чтобы эта рисовская полугруппа содержала менее 19 элементов, необходимо, чтобы сэндвич-матрица не содержала нулей (в этом случае полугруппа будет 18-элементной). Любую такую матрицу можно нормализовать к виду или $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, или $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & a \end{pmatrix}$, или $\begin{pmatrix} 1 & 1 & 1 \\ 1 & a & b \end{pmatrix}$. В первом случае соответствующая полугруппа легкая по следствию 4.1. Две другие полугруппы, хоть и не изоморфны, удовлетворяют одним и тем же тождествам. Условия выполнения тождеств в этих полугруппах полиномиально проверяемы, т. е. полугруппы опять-таки легкие. Оба последних результата можно найти в [22, 23].

Случай 5. Пусть сэндвич-матрица имеет размер 3×3. В таком случае для получения рисовской полугруппы, содержащей менее 19 элементов, структурная группа должна быть либо единичной, либо циклической второго порядка. Если структурная группа единична или сэндвич-матрица содержит лишь 0 и 1, то задача проверки тождеств в таких полугруппах полиномиально разрешима по следствию 4.1. Следовательно, мы с необходимостью приходим к рисовской матричной полугруппе над циклической группой $\mathbb{C}_2 = \{a, 1\}$ с сэндвич-матрицей, содержащей все три элемента $\{0, 1, a\}$, как к примеру минимальной 0-простой полугруппы, интересной с точки зрения сложности задачи проверки тождеств.

5. Графовые конструкции в задаче ID-CHECK($\mathcal{M}$)

Под *двудольным графом* понимается тройка (V, W, E), где V и W – непересекающиеся множества вершин графа (две доли графа), а E – множество ребер вида (v, w), где $v \in V$ и $w \in W$. Под *мультиграфами* понимаются графы с кратными ребрами: множество ребер E рассматривается как мультимножество, а кратностью ребра (v, w) соответственно называется мощность множества $\{e \in E\colon e = (v, w)\}$.

Под гомоморфизмом $\varphi\colon G \to G'$ мультиграфа $G = (V, W, E)$ на обыкновенный граф $G' = (V', W', E')$ мы будем понимать отображение множеств вершин $f\colon V \cup W \to V' \cup W'$, сохраняющее отношение «быть ребром» (из условия $(v, w) \in E$ следует, что $(f(v), f(w)) \in E'$).

Под *двудольным гомоморфизмом* $\varphi\colon G \to G'$ двудольного мультиграфа $G = (V, W, E)$ на обыкновенный граф $G' = (V', W', E')$ мы будем понимать гомоморфизм, сохраняющий отношение «принадлежать разным долям» (из условий $v \in V$ и $w \in W$ следует, что $f(v)$ и $f(w)$ принадлежат разным долям графа G').

Мы не приводим определение гомоморфизма мультиграфа на мультиграф, чтобы не уточнять возникающие в таком случае нюансы. В итоге в данной работе не различаются гомоморфизмы обыкновенных графов и мультиграфов. Однако для нас существенно рассмотрение именно двудольных гомоморфизмов, так как обыкновенный гомоморфизм в случае несвязности графа не гарантирует сохранение отношения «принадлежать разным долям».

Как было упомянуто ранее, для доказательства основного результата мы введем промежуточную задачу, касающуюся гомоморфизмов двудольных графов. Речь идет о следующей комбинаторной задаче распознавания для заданного двудольного графа H:

УСЛОВИЕ: двудольный мультиграф $\widetilde{G}$ с четными степенями всех вершин.

ВОПРОС: Верно ли, что для любого двудольного гомоморфизма графов $\varphi\colon \widetilde{G} \to H$ мощность прообраза каждого ребра графа H четна?

Мы будем называть эту задачу двудольной задачей о четных гомоморфизмах для графа H и обозначать ее через B-EVEN-HOM(H). Буква B в данном обозначении является сокращением слова bipartite и подчеркивает, что в задаче рассматриваются только двудольные графы и только двудольные гомоморфизмы. Если отказаться от условий двудольности, можно сформулировать «недвудольную» задачу о четных гомоморфизмах, которую имеет смысл обозначить через EVEN-HOM(H):

УСЛОВИЕ: мультиграф $\widetilde{G}$ с четными степенями всех вершин.

ВОПРОС: Верно ли, что для любого гомоморфизма $\varphi\colon \widetilde{G} \to H$ мощность прообраза каждого ребра графа H четна?

В разделах 5 и 8 мы будем рассматривать задачу B-EVEN-HOM(H), а в разделе 9 перейдем к рассмотрению задачи EVEN-HOM(H).

Для начала переведем задачу ID-CHECK($\mathcal{M}$) на язык двудольных графов. Определим двудольный граф $G(V, W, E)$, отвечающий полугруппе $\mathcal{M}$, следующим образом: $V = \{i_1, i_2, i_3\}, W = \{\lambda_1, \lambda_2, \lambda_3\}$ и $(\lambda_\ell, i_k) \in E$ тогда и только тогда, когда $P(\lambda_\ell, i_k) \neq 0$, т. е. тогда и только тогда, когда $\lambda_\ell \neq i_k$. Проведя построения, мы получаем граф шестиугольника; будем в дальнейшем обозначать его через Hex (рис. 1).

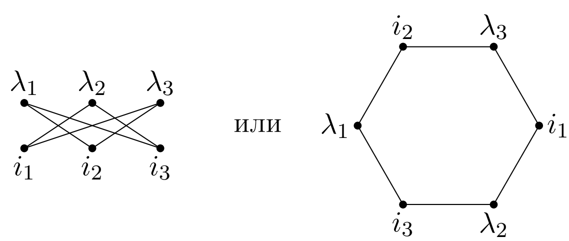


Рис. 1. Графы шестиугольника

Далее по произвольному слову p построим двудольный граф $G_p(V_p, W_p, E_p)$. Для этого по каждой переменной x_k слова p зададим две вершины $a_k \in V_p$ и $b_k \in W_p$; ребра построим по правилу: $(a_k, b_\ell) \in E_p$ тогда и только тогда, когда слово p содержит 2-фактор (подслово) $x_k x_\ell$.

Дополнительно для каждого слова p мы определим двудольный мультиграф $\widetilde{G}_p(V_p, W_p, E_p)$ следующим образом: каждому ребру (a_k, b_ℓ) обыкновенного графа $G_p(V_p, W_p, E_p)$ припишем кратность, равную числу появления фактора $x_k x_\ell$ в слове p.

Отметим, что описанные построения графов по данному слову полиномиально реализуемы.

Пример 5.1. Пусть дано слово $p = x_1 x_2 {x_1}^2 x_3 x_4 {x_5}^2 x_2 {x_1}^2 x_2 x_1 x_2$. На рис. 2 изображен соответствующий двудольный граф, а на рис. 3 – двудольный мультиграф.

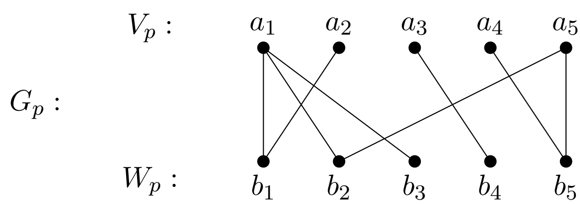


Рис. 2

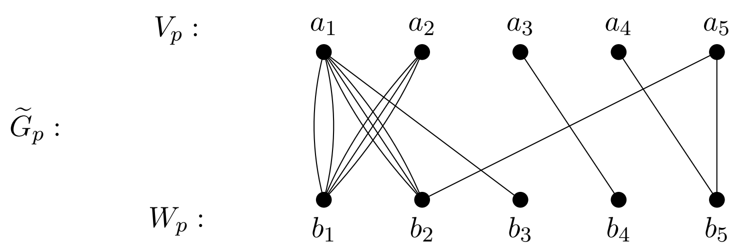


Рис. 3

6. Необходимые условия выполнения тождества в полугруппе $\mathcal{M}$

В этом разделе мы рассмотрим некоторые полезные свойства тождеств над полугруппой $\mathcal{M}$ и постепенно покажем тесную взаимосвязь задач ID-CHECK($\mathcal{M}$) и B-EVEN-HOM(Hex). Для сокращения записи договоримся через $\overline{p}$ обозначать результат подстановки элементов полугруппы $\mathcal{M}$ в p.

Пусть на входе задачи проверки тождеств в полугруппе $\mathcal{M}$ дано тождество $p \equiv q$, где $p = x_1 \dots x_n$ и $q = y_1 \dots y_m$. Через Σ обозначим алфавит слов p и q, считая, что в Σ нет «лишних» букв. Ниже перечислим необходимые условия выполнения тождества $p \equiv q$ в полугруппе $\mathcal{M}$.

Для начала отметим тот очевидный факт, что из выполнения некоторого тождества в полугруппе следует его выполнение и в произвольной подполугруппе данной полугруппы. В силу того, что исследуемая полугруппа $\mathcal{M}$ содержит ряд подполугрупп, условия выполнения тождеств в которых известны, непосредственным следствием этих результатов будет необходимость выполнения этих условий в самой полугруппе $\mathcal{M}$.

Для начала рассмотрим подполугруппу $\mathcal{M}/\mathcal{H}$ – факторизацию полугруппы $\mathcal{M}$ по отношению Грина $\mathcal{H}$ (см. раздел 2). Во введенных выше обозначениях тождество $p \equiv q$ выполнено в полугруппе $\mathcal{M}/\mathcal{H}$ тогда и только тогда, когда выполнены следующие два условия (см. [17, теорема 4.3]).

Условие 1. $G_p = G_q$.

Условие 2. $x_1 = y_1$, $x_n = y_m$.

Следующее замечание раскрывает внутренний смысл совпадения графов слов.

Замечание 6.1. *Два графа G_p и G_q совпадают тогда и только тогда, когда при любом означивании алфавита Σ в полугруппе $\mathcal{M}$ слова p и q могут обратиться в 0 только одновременно. В частности, задача проверки по двум данным словам их одновременного равенства 0 при любом означивании алфавита Σ в полугруппе $\mathcal{M}$ имеет полиномиальную сложность.*

Доказательство. В силу пункта (1) леммы 2.1 данное слово равно 0 в полугруппе $\mathcal{M}$ тогда и только тогда, когда оно равно 0 в полугруппе $\mathcal{M}/\mathcal{H}$. В свою очередь, слова одновременно обращаются в 0 при любом означивании в полугруппе $\mathcal{M}/\mathcal{H}$ тогда и только тогда, когда их графы совпадают [17, лемма 4.2]. При этом проверка совпадения двух данных обыкновенных графов реализуется за полиномиальное время от общего числа вершин, т. е. от мощности алфавита Σ.

Условие 3. Для каждой буквы x_k четность числа ее вхождений в левую и правую части тождества $p \equiv q$ одинакова.

Доказательство. Полугруппа $\mathcal{M}$ содержит подгруппы, изоморфные ее структурной группе $\mathbb{C}_2$, т. е. циклической группе второго порядка. Эти подгруппы имеют вид $\{(i, e, \lambda), (i, a, \lambda)\}$, где для пары (i, λ) выполняется условие $p_{\lambda i} \neq 0$. Условие 3 как раз и является необходимым и достаточным для выполнения тождества в группе $\mathbb{C}_2$.

Замечание 6.2. *В дальнейшем благодаря замечанию 6.1 будем рассматривать только такие означивания слов тождества элементами полугруппы $\mathcal{M}$, при которых $\overline{p} \neq 0$ и $\overline{q} \neq 0$.*

Более того, будем рассматривать только такие тождества, которые удовлетворяют ранее перечисленным необходимым условиям **1**, **2**, **3**, *так как эти условия проверяются за полиномиальное от $|\Sigma|$ время.*

Условие 4. При любом означивании слов тождества элементами полугруппы $\mathcal{M}$ четность числа стыков вида $\langle ., 2\rangle\langle 1,.\rangle$ одинакова для p и q.

Доказательство. По лемме 3.1 в результате ненулевого означивания слов тождество имеет вид $(i_1, a^k a^\ell, \lambda_n) = (i_1, a^{k'} a^{\ell'}, \lambda_n)$. Таким образом, тождество выполняется тогда и только тогда, когда $a^k a^\ell = a^{k'} a^{\ell'}$. Последнее верно тогда и только тогда, когда $k + \ell = k' + \ell' \pmod 2$. В силу условия **3** имеем $k = k' \pmod 2$, т. е. необходимым условием является $\ell = \ell' \pmod 2$. Что и требовалось доказать.

Теорема 6.1. *Условия* **1**, **2**, **3**, **4** *являются необходимыми и достаточными для выполнения тождества $p \equiv q$ в полугруппе $\mathcal{M}$.*

Доказательство. Необходимость была доказаны выше. Докажем достаточность. Пусть данное тождество $p \equiv q$ удовлетворяет условиям **1**, **2**, **3**. Покажем, что условие **4** будет достаточным для выполнения тождества в полугруппе $\mathcal{M}$.

Действительно, при любом означивании слов p и q они либо одновременно равны 0 (см. замечание 6.1), либо (см. лемму 3.1) имеют вид $(i_1, a^k a^\ell, \lambda_n)$ и $({i'}_1, a^{k'} a^{\ell'}, {\lambda'}_n)$. В силу условия **2** имеем $i_1 = {i'}_1$, $\lambda_n = {\lambda'}_n$. В силу условия **3** имеем $k = k' \pmod 2$. Таким образом, условие $\ell = \ell' \pmod 2$, т. е. совпадение четностей числа стыков вида $\langle ., 2\rangle\langle 1,.\rangle$ в словах p и q при любом означивании, является достаточным для выполнения тождества. Что и требовалось доказать.

Насколько нам известно, приведенное описание тождеств полугруппы $\mathcal{M}$ ранее не публиковалось, хотя близкое по смыслу (но сформулированное в других терминах) описание можно найти в работе Г. Машевицкого [25, предложение 4.3].

Следствие 6.1. *Пусть дано тождество $p \equiv q$, удовлетворяющее условиям* **1**, **2**, **3**. *При анализе сложности задачи* ID-CHECK($\mathcal{M}$) *мы можем проверять только подстановки вида $\langle i, \lambda \rangle$, не заботясь о значении группового (среднего) элемента.*

Доказательство. Из замечания 6.2 и рассуждений предыдущей теоремы 6.1 видно, что вся сложность задачи выполнимости тождеств в полугруппе $\mathcal{M}$ связана исключительно с четностью числа стыков вида $\langle ., 2\rangle\langle 1, .\rangle$ при означивании слова. При этом неважно, возьмем ли мы элемент (i, e, λ) или (i, a, λ). Равенство произведения нулю также зависит только от $\langle i, \lambda \rangle$, а не от группового (среднего) элемента.

7. Взаимосвязь задач ID-CHECK($\mathcal{M}$) и B-EVEN-HOM(Hex)

Как упоминалось ранее, мы хотим свести задачу о четных гомоморфизмах для двудольного графа-шестиугольника Hex (в дальнейшем просто шестиугольник) к задаче ID-CHECK($\mathcal{M}$). Поэтому теперь мы приступим к описанию задачи проверки тождеств на языке гомоморфизмов двудольных графов.

Для каждой ненулевой подстановки ε элементов полугруппы $\mathcal{M}$ в слово p мы можем определить отображения $\varphi_p \colon G_p \to Hex$ и $\widetilde{\varphi}_p \colon \widetilde{G}_p \to Hex$ по следующему правилу:

$$\text{если } \varepsilon(x_k) = \langle i, \lambda \rangle \text{ для буквы } x_k \in p,$$
$$\text{то } \varphi_p(a_k) = \widetilde{\varphi}_p(a_k) = \lambda \text{ и } \varphi_p(b_k) = \widetilde{\varphi}_p(b_k) = i. \quad (1)$$

Замечание 7.1. *Пусть дано слово p и некоторая ненулевая подстановка ε элементов полугруппы $\mathcal{M}$ в слово p. Тогда следующие условия эквивалентны:*

(1) *отображение φ_p является гомоморфизмом;*

(2) *отображение $\widetilde{\varphi}_p$ является гомоморфизмом;*

(3) $\varepsilon(p) \neq 0$.

Доказательство. Докажем эквивалентность условий (2) и (3) условию (1).

(1)⇔(2) Запишем требование гомоморфизма сохранения ребер: из того, что (a_k, b_j) является ребром в графе G_p [или $\widetilde{G}_p$], должно следовать, что $(\varphi_p(a_k), \varphi_p(b_j))$ [или $(\widetilde{\varphi}_p(a_k), \widetilde{\varphi}_p(b_j))$] является ребром в шестиугольнике Hex. Из определения очевидно, что для обоих отображений это условие выполняется одновременно.

(1)⇔(3) Для доказательства гомоморфности отображения φ_p необходимо проверить, что из того, что (a_k, b_j) является ребром в графе G_p, следует, что $(\varphi_p(a_k), \varphi_p(b_j))$ является ребром в шестиугольнике Hex. Действительно, (a_k, b_j) является ребром в графе G_p тогда и только тогда, когда существует 2-фактор $x_k x_j$ в слове p. В свою очередь, $x_k x_j$ не обращается в 0 при означивании букв элементами $\langle i, \lambda\rangle$ и $\langle i', \lambda'\rangle$ тогда и только тогда, когда $p_{\lambda i'} \neq 0$, т. е. тогда и только тогда, когда существует ребро (λ, i') в графе-шестиугольнике Hex. Отображение φ_p мы построили таким образом, что $(\varphi_p(a_k), \varphi_p(b_j)) = (\lambda, i')$. Вспомним, что для ненулевой подстановки ε имеем $\varepsilon(p) = 0$ тогда и только тогда, когда в ноль обращается какой-нибудь из 2-факторов слова p. Теперь совсем не сложно понять, что из $(a_k, b_j) \in E(G_p)$ следует $(\varphi_p(a_k), \varphi_p(b_j)) \in E(Hex)$ тогда и только тогда, когда $\varepsilon(p) \neq 0$. Что и требовалось доказать.

Так как мы договорились действовать в рамках замечания 6.2, то все рассматриваемые нами означивания слов могут быть представлены конструкцией гомоморфизмов (1). Следующее замечание дает обратное соответствие.

Замечание 7.2. *Пусть дано слово p и по нему построен граф $\widetilde{G}_p$. Тогда для произвольного двудольного гомоморфизма $\widetilde{\varphi}\colon \widetilde{G}_p \to Hex$ найдется такая подстановка ε элементов полугруппы $\mathcal{M}$ в слово p, что гомоморфизм графа $\widetilde{G}_p$, построенный по ε в соответствии с формулой* (1)*, в точности совпадет с данным $\widetilde{\varphi}$.*

Доказательство. Без ограничения общности (в силу симметрии обеих долей шестиугольника Hex) считаем, что доля $\{a_1, \dots a_n\}$ графа $\widetilde{G}_p$ перейдет в долю $\{\lambda_1, \lambda_2, \lambda_3\}$ шестиугольника Hex. При этом доля $\{b_1, \dots b_n\}$ обязательно перейдет в долю $\{i_1, i_2, i_3\}$. Предположим, что $\widetilde{\varphi}(a_k) = \lambda$ и $\widetilde{\varphi}(b_k) = i$. Тогда положим $\varepsilon(x_k) = \langle i, \lambda\rangle$ для соответствующей буквы x_k. Таким образом, мы определили подстановку ε с требуемыми условиями.

Теперь речь можно вести не о произвольной подстановке элементов полугруппы $\mathcal{M}$, а о произвольном двудольном гомоморфизме графов в граф шестиугольника.

Для прояснения конструкции (1) рассмотрим подслово $x_i x_k x_j$. Предположим, что мы произвели некоторое означивание букв ненулевыми элементами полугруппы $\mathcal{M}$. Тогда при вычислении значения данного подслова нам будут интересны именно стыки означенных букв (см. следствие 6.1). А именно если имеем $\overline{x_i x_k x_j} = \langle i_1, \lambda_1\rangle\langle i_2, \lambda_2\rangle\langle i_3, \lambda_3\rangle$, то анализ значения переменной x_k при нахождении результата подстановки в данный 3-фактор будет заключаться лишь в проверке следующих четырех условий: $p_{\lambda_1 i_2} = 0$, $p_{\lambda_2 i_3} = 0$, $p_{\lambda_1 i_2} = a$ и $p_{\lambda_2 i_3} = a$. Если ни одно из этих условий не выполняется, то результат подстановки тривиален, так как зависит лишь от i_1 и λ_3.

Если вспомнить строение графов G_p и $\widetilde{G}_p$ по слову p, то легко заметить, что ребра этих графов отвечают как раз стыкам букв, т. е. стык $x_i x_k$ есть тогда и только тогда, когда есть ребро $a_i b_k$. Именно поэтому представляется естественным рассматривать стык букв, выраженный ребром $a_i b_k$, как стык означивания, выраженный парой (λ_1, i_2). Поэтому доля графов G_p и $\widetilde{G}_p$, содержащая элементы a_i, отображается в долю графа Hex, содержащую λ_i. Фактически конструкция довольно прозрачна: просто каждое ребро графов G_p и $\widetilde{G}_p$ мы означиваем ребром шестиугольника Hex.

Мультиграфы $\widetilde{G}_p$ и $\widetilde{G}_q$ можно рассматривать как мультимножества, элементами которых являются ребра с соответствующей кратностью. Приняв такую позицию, можно построить объединение в смысле мультимножеств и тем самым получить мультиграф $\widetilde{UG} = (V_p, W_p, \widetilde{E}_p \uplus \widetilde{E}_q)$, где $\widetilde{E}_p \uplus \widetilde{E}_q$ – это объединение ребер в смысле мультимножеств, т. е. состоит из множества всех ребер $E_p \cup E_q$ в качестве носителя, и при этом каждое ребро получает кратность, равную сумме его кратностей в мультиграфах $\widetilde{G}_p$ и $\widetilde{G}_q$.

Пример 7.1. Пусть дано слово $q = {x_1}^2 x_2 x_1 x_3 x_4 {x_5}^4 x_2$. Слово p возьмем из примера 5.1. Тогда:

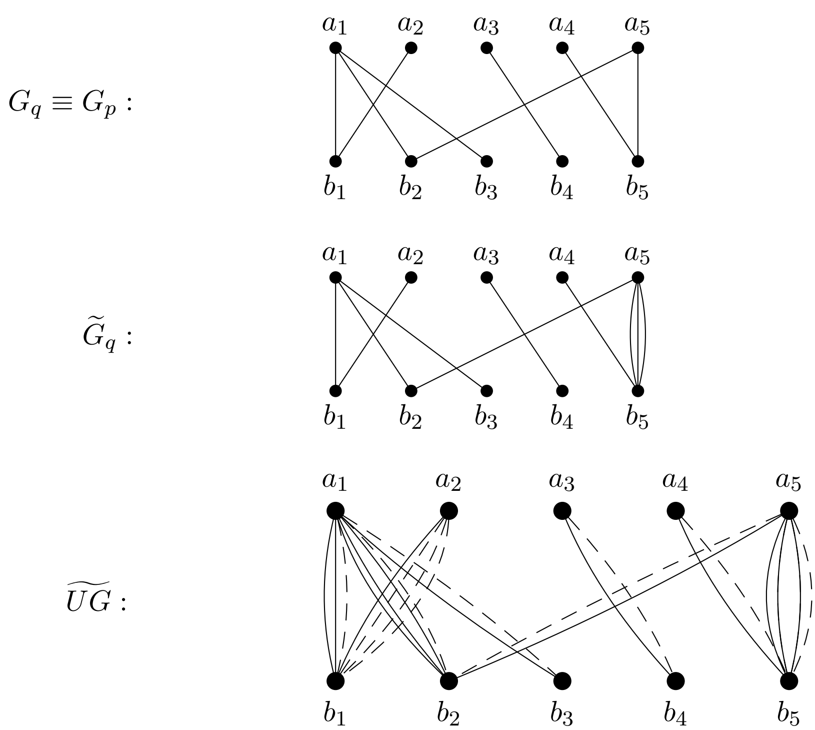


Рис. 4

Далее мы приведем условия, эквивалентные условиям **3**, **4**.

Условие 3′. Степень каждой вершины графа $\widetilde{UG}$ четна.

Доказательство. Для начала заметим, что условие **3** можно переформулировать следующим образом: для каждой вершины графа $\widetilde{G}_p$ аналогичная вершина (отвечающая той же букве алфавита и в той же доле) в графе $\widetilde{G}_q$ имеет степень такой же четности. Отсюда и из определения мультиграфа $\widetilde{UG}$ немедленно следует эквивалентность условий **3** и **3′**.

Условие 4′. Для произвольного двудольного гомоморфизма $\varphi\colon \widetilde{UG} \to Hex$ каждое ребро $(\lambda, i) \in Hex$ имеет четный по мощности прообраз, т. е.

$$|\varphi^{-1}(\lambda, i)| = 0 \mod 2.$$

Доказательство. Прежде всего напомним, что мультиграфы $\widetilde{G}_p$, $\widetilde{G}_q$ и $\widetilde{UG}$ совпадают как обыкновенные графы (если кратностям всех ребер приписать единицу). Следовательно, гомоморфизм φ можно рассматривать как гомоморфизм графов $\widetilde{G}_p$ и $\widetilde{G}_q$. При этом замечания 7.1 и 7.2 устанавливают взаимнооднозначное соответствие между произвольными двудольными гомоморфизмами в граф шестиугольника и означиваниями слов в полугруппе $\mathcal{M}$. Отсюда, благодаря конструкции (1), условие **4** можно переформулировать следующим образом: для произвольного двудольного гомоморфизма $\varphi\colon \widetilde{UG} \to Hex$ выполнено условие $|\varphi_{|_{G_p}}{}^{-1}(\lambda_2, i_1)| = |\varphi_{|_{G_q}}{}^{-1}(\lambda_2, i_1)| \mod 2$. Однако в силу поворотной симметрии шестиугольника мы можем легко перевести произвольное ребро (λ, i) в ребро (λ_2, i_1), тем самым получив какой-то другой двудольный гомоморфизм, а вместе с тем и условие о совпадении четностей прообразов. Следовательно, для произвольного двудольного гомоморфизма $\varphi\colon \widetilde{UG} \to Hex$ и для любого ребра $(\lambda, i) \in Hex$ выполнено условие $|\varphi_{|_{G_p}}{}^{-1}(\lambda, i)| = |\varphi_{|_{G_q}}{}^{-1}(\lambda, i)| \mod 2$, что, в свою очередь, эквивалентно условию $|\varphi^{-1}(\lambda, i)| = 0 \mod 2$.

Замечание 7.3. *Из условия* **4′** *следует выполнение условия* **3′**.

Доказательство. От противного. Пусть мы имеем хотя бы одну вершину нечетной степени. Без ограничения общности пусть эта вершина принадлежит $\widetilde{V}$. Тогда мы построим такой двудольный гомоморфизм, который выбранную вершину нечетной степени отправляет в λ_3, любую другую вершину из $\widetilde{V}$ отправляет в λ_1, а любую вершину из $\widetilde{W}$ отправляет в i_2. Это можно сделать, соблюдая условие гомоморфности отображения (см. строение двудольного графа шестиугольника). Описанный гомоморфизм не является четным по нашему определению, так как прообраз ребра (λ_3, i_2), очевидно, получился нечетным по мощности. Пришли к противоречию с 4′.

Следствие 7.1. *Условия* **1, 2, 4′** *являются необходимыми и достаточными для выполнения тождества* $p \equiv q$ *в полугруппе* $\mathcal{M}$.

Мы уже отмечали, что именно с условием **4** (а значит, и **4′**) связана вся сложность задачи ID-CHECK($\mathcal{M}$). Поэтому оно столь важно в нашем исследовании и заслуживает аккуратного рассмотрения. Ниже мы приведем утверждения, позволяющие переходить от одного мультиграфа к другому, сохраняя для них одновременное удовлетворение условию **4′**.

Доказательство следующей леммы весьма несложное и следует непосредственно из формулировки условия **4′**.

Лемма 7.1. *Пусть даны двудольные мультиграфы* $\widetilde{G}$ *и* $\widetilde{G}_1$ *такие, что соответствующие им обыкновенные графы* G *и* G_1 *совпадают. Если для каждого ребра графа* $G = G_1$ *четность его кратности совпадает в* $\widetilde{G}$ *и* $\widetilde{G}_1$, *то графы* $\widetilde{G}$ *и* $\widetilde{G}_1$ *удовлетворяют условию* **4′** *одновременно.*

Лемма 7.1 перестает быть верной, если убрать требование совпадения обыкновенных графов: в общем случае не верно, что ребра нулевой кратности можно заменить на ребра с четной кратностью с сохранением условия **4′**.

Лемма 7.2. *Пусть дан двудольный граф* $\widetilde{G}$, *имеющий изолированные вершины. Пусть граф* $\widetilde{G}_1$ *получен из исходного добавлением новых четных по кратности ребер, соединяющих изолированные вершины с неизолированными так, что каждая изолированная вершина смежна максимум с одной неизолированной. Тогда графы* $\widetilde{G}$ *и* $\widetilde{G}_1$ *удовлетворяют условию* **4′** *одновременно.*

Доказательство. Без ограничения общности предположим, что изолированные вершины графа $\widetilde{G}$, соединенные новыми ребрами в графе $\widetilde{G}_1$, принадлежат верхней доле. Через e_s для $s \in \{1, \dots, \ell\}$ обозначим упомянутые новые ребра в графе $\widetilde{G}_1$. Докажем, что свойство **4′** выполнено для графов $\widetilde{G}$ и $\widetilde{G}_1$ одновременно.

Пусть свойство **4′** выполнено для графа $\widetilde{G}_1$. Рассмотрим произвольный гомоморфизм φ графа $\widetilde{G}$ на шестиугольник Hex и его действие на графе $\widetilde{G}_1$. Есть две возможности: данное вершинное отображение на графе $\widetilde{G}_1$ является или не является гомоморфизмом. Если свойство гомоморфности сохранилось, то при этом ребра e_s перейдут в некоторые ребра (λ, i). Это значит, что в графе $\widetilde{G}_1$ прообраз ребра (λ, i) увеличился на число, кратное 2, а значит, остался четным. Следовательно, свойство **4′** выполнено и для графа $\widetilde{G}$.

Иначе, пусть φ, рассмотренный как вершинное отображение на графе $\widetilde{G}_1$, не является гомоморфизмом. Это может произойти в том случае, если вершины ребер e_s перейдут в несмежные вершины шестиугольника Hex, однако обязательно лежащие в разных долях (т. е. ребро e_s отобразится на несуществующее ребро (λ_k, i_k)). Изменим φ таким образом, чтобы образом ребра e_s стало ребро шестиугольника (λ_{k+1}, i_k) или (λ_{k-1}, i_k), т. е. «передвинем» образ ребра e_s на существующее в шестиугольнике ребро. Такую операцию мы сможем проделать для всех новых ребер e_s. Тем самым мы получим φ – гомоморфизм графа $\widetilde{G}_1$. Мощность прообраза каждого ребра вида (λ_{k+1}, i_k) или (λ_{k-1}, i_k) увеличится на четное число – на кратности ребер e_s, мощности всех остальных ребер не изменятся. По условию все прообразы четны, значит, свойство $\mathbf{4'}$ выполнено и для графа $\widetilde{G}$.

Обратно, пусть свойство $\mathbf{4'}$ выполнено для графа $\widetilde{G}$. Пусть при некотором гомоморфизме графа $\widetilde{G}_1$ ребро e_s переходит в ребро (λ, i). Любой гомоморфизм графа $\widetilde{G}_1$, очевидно, является гомоморфизмом графа $\widetilde{G}$. Тогда при том же гомоморфизме для графа $\widetilde{G}$ прообраз ребра (λ, i) уменьшится на четное число, т. е. останется четным. Значит, свойство $\mathbf{4'}$ выполнено и для графа $\widetilde{G}_1$.

Изолированные вершины нижней доли рассматриваются аналогично.

Для удобства будем называть двудольный граф $G = (V, W, E)$ *равнодольным*, если выполнено равенство $|V| = |W|$.

Следствие 7.2. *Ограничение задачи* B-EVEN-HOM(Hex) *на равнодольные графы не умалит ее сложности.*

Доказательство. Для доказательства необходимо свести общую задачу B-EVEN-HOM(Hex) к ее ограничению на равнодольные графы. Для этого по каждому данному двудольному графу построим его равнодольную копию, дополнив меньшую долю изолированными вершинами и соединив их двукратными ребрами с произвольной вершиной противоположной доли. Далее воспользуемся леммой 7.2.

Везде далее под равнодольностью графа, кроме равенства мощностей долей, будем понимать отсутствие изолированных вершин.

8. Сведение задачи B-EVEN-HOM(Hex) к задаче ID-CHECK($\mathcal{M}$)

Пусть $|V| = |W| = n$, при этом каждой вершине в верхней и нижней доле присвоен свой порядковый номер от 1 до n. Тогда вершину $b_i \in W$ назовем *соответствующей* вершине $a_i \in V$.

Основным инструментом сводимости будет полиномиальный алгоритм построения по данному равнодольному графу $\widetilde{G}(V, W, E)$ нового равнодольного графа $\widetilde{G}_1(V, W, E_1)$, для которого выполнено равенство степеней соответствующих вершин. Отметим, что все действия с графами будут производиться таким образом, чтобы сохранить выполнение свойства **4′**. При этом алгоритм будет использовать всего две операции: перестановку вершин в долях (фактически перенумерацию) и приписывание существующим ребрам дополнительной кратности. Для удобства, в силу леммы 7.1, будем предполагать, что в исходном мультиграфе $\widetilde{G}$ кратности ребер равны либо 1, либо 2.

Введем ряд определений, потребующихся нам для описания алгоритма.

Вершину b_i [a_i] назовем *голодной* в данном графе $\widetilde{G}$, если

$$deg(b_i) < deg(a_i) \qquad [\ deg(a_i) < deg(b_i)\ ].$$

Величину $deg(a_i) - deg(b_i)$ [$deg(b_i) - deg(a_i)$] назовем *голодом* вершины b_i [a_i]. Назовем пару (a_i, b_i) *уравновешенной*, если $deg(a_i) = deg(b_i)$.

Чередующейся цепью в графе $\widetilde{G}$ от вершины b_i до вершины a_k назовем цепь $b_i = b_{\ell_1} a_{\ell_2} b_{\ell_2} \ldots a_{\ell_n} b_{\ell_n} a_{\ell_{n+1}} = a_k$, в которой $(b_{\ell_j}, a_{\ell_{j+1}}) \in E$. Другими словами, чередующаяся цепь, начинаясь в вершине $b_i = b_{\ell_1}$, проходит по некоторому ребру (b_{ℓ_1}, a_{ℓ_2}) графа $\widetilde{G}$, затем спускается в соответствующую вершине a_{ℓ_2} вершину b_{ℓ_2} и дальше вновь идет по ребру графа $\widetilde{G}$ и т. д. Чередующаяся цепь с началом в вершине a_i определяется симметричным образом, т. е. это цепь вида $a_i = a_{\ell_1} b_{\ell_2} a_{\ell_2} \ldots b_{\ell_n} a_{\ell_n} b_{\ell_{n+1}} = b_k$, в которой $(a_{\ell_j}, b_{\ell_{j+1}}) \in E$.

Термин «чередование» появился в определении благодаря аналогии с алгоритмом поиска наибольшего паросочетания, в котором поиск в ширину проходит сначала по насыщенным в текущем паросочетании ребрам, а затем «возвращается» по ненасыщенным. В нашем случае имеются, с одной стороны, существующие ребра исходного графа, а с другой – мыслимые «возвращающиеся» ребра вида (a_{ℓ_j}, b_{ℓ_j}) (см. рис. 5).

Лемма 8.1. *В произвольном равнодольном мультиграфе $\widetilde{G}(V, W, E)$ для произвольной голодной вершины x существует чередующаяся цепь с началом в x, проходящая через вершину неуравновешенной пары, отличную от x.*

Доказательство. Как обычно, предполагаем, что вершины графа в долях занумерованы; через a_i будем обозначать вершины верхней доли, через b_i – вершины нижней доли. Без ограничения общности считаем, что $x = b_i$ для некоторого i.

Докажем от противного существование такой чередующейся цепи. Запустим из b_i поиск в ширину чередующейся цепи до голодной вершины a_k, используя метки пройденных вершин. Пусть все найденные поиском чередующиеся цепи содержат только вершины, принадлежащие уравновешенным парам.

Через V_1 обозначим множество помеченных в результате поиска вершин. Рассмотрим подграф G_1 исходного графа, *порожденный* множеством V_1, т. е.

подграф, содержащий все ребра вида (v, w) для $v, w \in V_1$. Обозначим через $deg'(v)$ степень вершины v в подграфе G_1. В силу определения чередующейся цепи степени вершин b_{ℓ_j} в данном подграфе G_1 совпадают с их полными степенями в графе $\widetilde{G}$, т. е. $deg'(b_{\ell_j}) = deg(b_{\ell_j})$, однако $deg'(a_{\ell_j}) \leq deg(a_{\ell_j})$. По предположению $deg(a_{\ell_j}) = deg(b_{\ell_j})$ для всех пар вершин, попавших в поиск, кроме исходной пары (a_i, b_i). Значит, $deg'(b_{\ell_j}) \geq deg'(a_{\ell_j})$ для всех пар подграфа G_1, кроме пары (a_i, b_i). Докажем, что $deg'(a_i) \geq deg(b_i)$.

Предположим, что $deg'(a_i) < deg(b_i)$, т. е. $deg'(a_i) < deg'(b_i)$. Тогда в подграфе G_1 найдется такая пара вершин (a_{ℓ_j}, b_{ℓ_j}), что $deg'(b_{\ell_j}) < deg'(a_{\ell_j})$, что невозможно. Отсюда $deg'(a_i) \geq deg(b_i)$, и, значит, $deg'(a_i) \neq 0$, а это эквивалентно тому, что некоторая чередующаяся цепь пройдет через вершину a_i. Однако, по условию, пара (a_i, b_i) является неуравновешенной. Противоречие.

Для краткости назовем два графа *эквивалентными* в смысле выполнения условия $\mathbf{4'}$, если эти графы удовлетворяют условию $\mathbf{4'}$ одновременно.

Лемма 8.2. *Для произвольного равнодольного графа G с четными степенями всех вершин существует полиномиальный от числа вершин алгоритм, строящий новый граф G_1 со следующими свойствами:*

(1) *все пары вершин графа G_1 уравновешены;*

(2) *граф G_1 эквивалентен графу G в смысле выполнения условия $\mathbf{4'}$.*

Доказательство. Мы будем проводить построение нового графа с помощью операций перестановки вершин и увеличения кратностей существующих ребер на 2. По лемме 7.1 полученный таким образом новый граф G_1 будет эквивалентен графу G в смысле выполнения свойства $\mathbf{4'}$. При этом, так как разность степеней вершин кратна 2, любой голод может быть утолен 2-кратными ребрами.

Основной идеей алгоритма будет насыщение неуравновешенных пар вдоль чередующихся цепей от голодной вершины в одной доле до голодной вершины в другой доле. Процедуру насыщения вдоль цепи

$$b_i = b_{\ell_1} a_{\ell_2} b_{\ell_2} \ldots a_{\ell_n} b_{\ell_n} a_{\ell_{n+1}} = a_k$$

на величину A можно описать следующим образом: увеличиваем степени всех вершин цепи, начиная с b_i, на величину A с помощью добавления кратности ребрам вида $(b_{\ell_j}, a_{\ell_{j+1}})$, вошедшим в данную цепь. Заметим, что при таком добавлении ребер величина $deg(a_{\ell_j}) - deg(b_{\ell_j})$ не изменится для всех пар вершин, входящих в цепь.

Шаг 1. Упорядочиваем обе доли графа G по возрастанию степеней вершин. Получившиеся пары вершин за линейное время можно разбить на два множества: уравновешенные пары и неуравновешенные пары. Если множество неуравновешенных пар не пусто, то переходим на шаг 2.

Шаг 2. Заново упорядочиваем обе доли вершин в неуравновешенной части по возрастанию их степеней. Заметим, что степени вершин в нижней и верхней долях попарно не равны, иначе бы такая пара равных вершин попала в уравновешенную часть.

Находим, в какой доле неуравновешенной части находится вершина с максимальной степенью. Без ограничения общности, пусть это вершина b_t. Очевидно, что выполнено неравенство $deg(a_t) < deg(b_t)$. Тогда в нижней доле обязательно существует некоторая голодная вершина b_i.

Начинаем из вершины b_i поиск в ширину чередующихся цепей до некоторой голодной a_k, используя метки пройденных вершин. Поиск в ширину остановится либо когда будет найдена голодная вершина a_k, либо когда не останется непройденных смежных вершин.

Шаг 2.1. Если голодная вершина a_k найдена, то вдоль построенной чередующейся цепи насыщаем вершины b_i и a_k на величину, равную минимуму их голода. Таким образом, хотя бы одна из пар (a_i, b_i) и (a_k, b_k) станет уравновешенной, при этом в силу определения процедуры насыщения вершин вдоль чередующейся цепи никакая другая пара своей уравновешенности не утратит.

Шаг 2.2. Пусть поиск в ширину отработал, но голодной вершины a_k найдено не было. По лемме 8.1 в произведенном поиске в ширину существует неуравновешенная пара (a_s, b_s). Рассмотрим чередующуюся цепь W от вершины b_i до вершины a_s. По предположению a_s не является голодной, следовательно, $s < t$, где t – номер найденной в начале шага 2 вершины с максимальной степенью. В силу проведенного в начале шага 2 упорядочения вершин по возрастанию их степеней можно заключить, что $deg(a_s) \leq deg(a_t)$.

Меняем местами вершины a_s и a_t. При этом вершина b_i останется голодной, новая вершина a_t (бывшая a_s) останется голодной, а чередующаяся цепь W соединит b_i с голодной a_t.

Насыщаем голодные вершины вдоль чередующейся цепи W.

Во множество уравновешенных пар добавляем только что полученные. Если множество неуравновешенных пар не пусто, то возвращаемся на шаг 2.

Алгоритм, очевидно, является полиномиальным от числа вершин исходного графа. Он конечен, так как в конце каждого выполнения шага 2 мы уменьшаем хотя бы на единицу мощность множества неуравновешенных пар. На выходе алгоритм даст граф G_1, удовлетворяющий обоим заявленным в лемме условиям.

Теорема 8.1 (теорема сводимости). *Дан двудольный граф шестиугольника Hex. Тогда для каждого связного двудольного мультиграфа $\widetilde{G}(V, W, \widetilde{E})$ с равными по мощности долями $|V| = |W|$ и с четными степенями всех вершин существуют такие слова p и q, удовлетворяющие условиям* **1** *и* **2**, *что $p \equiv q$ тогда и только тогда, когда для любого двудольного гомоморфизма $\varphi\colon \widetilde{G} \to Hex$ мощность прообраза каждого ребра шестиугольника Hex четна.*

Доказательство. По данному графу $\widetilde{G}$ с помощью алгоритма, приведенного в лемме 8.2, построим новый равнодольный граф $\widetilde{G}_1$ с четными степенями всех вершин и эквивалентный графу $\widetilde{G}$ в смысле выполнения свойства $\mathbf{4'}$.

Новый граф $\widetilde{G}_1$ будет обладать свойством попарного равенства степеней соответствующих вершин, т. е. $deg(a_i) = deg(b_i)$ для всех пар вершин (a_i, b_i). Мысленно дополним граф $\widetilde{G}_1$ специальными *возвращающимися* ребрами вида (b_i, a_i) и с кратностью, равной $deg(b_i)$; а всем существующим ребрам припишем ориентацию (a_i, b_j), т. е. будем считать их исходящими из вершин верхней доли (рис. 5). При такой ориентации любой ориентированный путь из некоторой вершины верхней доли a_i в графе $\widetilde{G}_1$ будет в точности совпадать с определенной выше чередующейся цепью из вершины a_i.

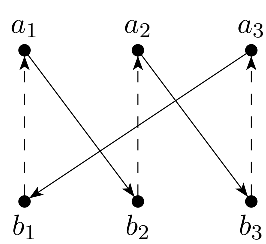


Рис. 5

Степень захода $\overrightarrow{deg}(b_i)$ для каждой вершины нижней доли совпадает с исходной степенью $deg(b_i)$ в графе $\widetilde{G}_1$, а степень исхода $\overleftarrow{deg}(b_i)$ совпадает с количеством мыслимых возвращающихся ребер, т. е. по определению также равна $deg(b_i)$. Степень исхода $\overleftarrow{deg}(a_i)$ для каждой вершины верхней доли совпадает с исходной степенью $deg(a_i)$ в графе $\widetilde{G}_1$, а степень захода $\overrightarrow{deg}(a_i)$

совпадает с количеством возвращающихся ребер (b_i, a_i), т. е. равна $deg(b_i)$. Так как $deg(a_i) = deg(b_i)$ для всех пар вершин (a_i, b_i), то в заданной ориентации степень исхода равна степени захода для каждой вершины графа $\widetilde{G}_1$. Следовательно, в силу связности графа $\widetilde{G}_1$, имеем существование эйлерова ориентированного цикла.

Эйлеров цикл можно рассматривать как прочтение слова вдоль ребер, если приписать всем парам вершин графа $\widetilde{G}_1$ некоторые буквы. Например, для циклического слова $p = x_1x_2x_3x_1x_3x_1$ мы имеем следующий граф $\widetilde{G}_p$, дополненный возвращающимися ребрами (рис. 6). Ориентированный цикл, отвечающий прочтению слова p, представляет из себя замкнутую чередующуюся цепь из вершины a_1.

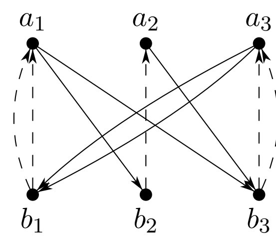


Рис. 6

По обходу графа $\widetilde{G}_1$ построим слова p и q, удовлетворяющие условиям **1** и **2**, и такие, что $p \equiv q$ тогда и только тогда, когда для любого двудольного гомоморфизма $\varphi\colon \widetilde{G}_1 \to Hex$ мощность прообраза каждого ребра шестиугольника Hex четна.

Обозначим через xAx – слово, читающееся вдоль эйлерова обхода графа $\widetilde{G}_1$. Тогда положим

$$p = xAx,$$

$$q = xAxAx.$$

Полученные слова, очевидно, удовлетворяют условию **1**. При этом их графы $\widetilde{G}_p$ и $\widetilde{G}_q$ совпадают между собой как множества ребер, но отличаются как мультимножества. А именно в графе $\widetilde{G}_p$ кратности всех ребер будут совпадать с их кратностями в графе $\widetilde{G}_1$. В графе $\widetilde{G}_q$ кратности всех ребер будут удвоены по сравнению с графом $\widetilde{G}_1$. Таким образом, слова p и q удовлетворяют условию **2**. При этом если по графам $\widetilde{G}_p$ и $\widetilde{G}_q$ построить их объединение – граф $\widetilde{UG}$, то все вершины в полученном графе будут иметь четные степени, а кратность ребер совпадать по четности с графом $\widetilde{G}_1$.

Тождество $p \equiv q$ выполняется тогда и только тогда, когда выполнено условие **4′** для графа $\widetilde{UG}$, а это в силу леммы 7.1 эквивалентно выполнению условия **4′** для графа $\widetilde{G}_1$, а значит, и для исходного графа $\widetilde{G}$. Отсюда получаем, что $p \equiv q$ тогда и только тогда, когда для любого двудольного гомоморфизма $\varphi\colon \widetilde{G} \to Hex$ мощность прообраза каждого ребра шестиугольника Hex четна. Что и требовалось доказать для построенных слов p и q.

Итак, доказав приведенную теорему, мы тем самым полиномиально свели задачу B-EVEN-HOM(Hex), ограниченную на связных графах, к задаче ID-CHECK($\mathcal{M}$).

9. Взаимосвязь задачи о ретракции графов, задачи EVEN-HOM и задачи B-EVEN-HOM

В этом разделе мы докажем coNP-полноту ограничений на связные графы задач B-EVEN-HOM(Hex) и EVEN-HOM(Hex), откуда немедленно будет следовать и coNP-полнота самих задач, и coNP-полнота задачи ID-CHECK($\mathcal{M}$).

Для краткости условимся называть прообраз ребра четным или нечетным, подразумевая под этим четность или нечетность мощности прообраза. Будем называть гомоморфизм φ графа $\widetilde{G}$ в шестиугольник Hex *нечетным*, если существует такое ребро в графе Hex, что его прообраз в графе $\widetilde{G}$ при данном гомоморфизме φ является нечетным (отрицание четности гомоморфизма).

Так как по теореме 2.1 и предложению 2.2 задача RET(Hex), даже ограниченная на связных графах, NP-полна, то из приводимой ниже теоремы немедленно следует coNP-полнота задачи EVEN-HOM(Hex).

Теорема 9.1. *Задача ретракции* RET(Hex) *для шестиугольника Hex, ограниченная на связных графах, полиномиально сводима к отрицанию задачи* EVEN-HOM(Hex).

Доказательство. По произвольному связному графу B, содержащему в качестве подграфа шестиугольник H, мы построим связный граф $\widetilde{B}$ с четными степенями всех вершин такой, что ретракция $\varphi\colon B \to H$ существует тогда и только тогда, когда существует нечетный гомоморфизм $\psi\colon \widetilde{B} \to Hex$.

Для построения графа $\widetilde{B}$ мы удвоим кратность каждого ребра исходного графа B за исключением ребер, принадлежащих подграфу H. Степени каждой вершины полученного графа, безусловно, будут четны.

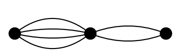
Заметим, что необходимость существования нечетного гомоморфизма достаточно очевидна. Ретракция графа B существует тогда и только тогда, когда существует такая же ретракция графа $\widetilde{B}$, так как гомоморфизм – это вершинное отображение. При этом ретракция $\varphi\colon \widetilde{B} \to H$ является нечетным гомоморфизмом в силу нашего построения, так как прообраз каждого ребра шестиугольника состоит из некоторого количества удвоенных ребер графа

$\widetilde{B}$ и ровно одного ребра графа H. Таким образом, для получения искомого нечетного гомоморфизма остается лишь организовать тождественный гомоморфизм $\varepsilon\colon H \to Hex$. Отметим, что в общем случае $H \neq Hex$, так как H – это подграф графа B, а Hex – произвольный граф шестиугольника.

Для доказательства достаточности мы покажем, что каждый нечетный гомоморфизм $\psi\colon \widetilde{B} \to Hex$ действует на $H \to Hex$ как сюръекция (а значит, является изоморфизмом), т. е. оставляет шестиугольник H шестиугольником. Из этого будет следовать существование ретракции $\varphi\colon \widetilde{B} \to H$, а значит, и ретракции $\varphi\colon B \to H$, которая может быть получена в виде $\varphi = \psi \circ \psi|_H{}^{-1}$.

Докажем от противного. Пусть некоторый нечетный гомоморфизм ψ не сохраняет H как шестиугольник, т. е. образ H не равен Hex. Для получения противоречия докажем, что такой гомоморфизм не может быть нечетным. Заметим, что в силу построения графа $\widetilde{B}$ все его ребра, за исключением ребер подграфа H, дают четный вклад в прообраз каждого ребра шестиугольника Hex. Это наблюдение позволяет нам ограничить рассмотрение исходного гомоморфизма ψ лишь его действием на H.

Как нетрудно видеть, образом любого гомоморфизма шестиугольника в себя является либо он сам, либо одно ребро, либо путь длины 2 или 3. В первом случае результат следует немедленно. Во втором случае кратность ребра равна 6, а значит, такой гомоморфизм четен. Для получения противоречия в последнем случае заметим, что при «склеивании» вершин шестиугольника четность степени каждой вершины есть инвариант. Тогда распределение кратностей ребер в путях длины 2 и 3 может быть только следующим:

 и 

Пришли к противоречию с нечетностью соответствующего гомоморфизма.

Следовательно, любой нечетный гомоморфизм $\psi\colon \widetilde{B} \to Hex$ действует на $H \to Hex$ как сюръекция. Следовательно, благодаря проведенным выше рассуждениям, мы доказали существование ретракции $\varphi\colon B \to H$.

Нетрудно заметить, что проведенные в теореме построения фактически ограничивают задачу EVEN-HOM(Hex) на связные графы.

Замечание 9.1. *Ограничение задачи* EVEN-HOM(Hex) *на связные графы не умаляет ее сложности.*

Следующим шагом мы сведем задачу EVEN-HOM(Hex) к задаче B-EVEN-HOM(Hex).

Замечание 9.2. *Ограничение задачи* EVEN-HOM(Hex) *на двудольные графы не умаляет ее сложности.*

Доказательство. Утверждение немедленно следует из хорошо известного и довольно тривиального факта, что для недвудольных графов не существует гомоморфизма на двудольный граф.

Теорема 9.2. *Задача* B-EVEN-HOM(Hex) coNP-*полна.*

Доказательство. Заметим, что, будучи ограниченными на связные двудольные графы, задачи EVEN-HOM(Hex) и B-EVEN-HOM(Hex) в точности совпадают, в частности, потому, что на связных графах совпадают двудольные и обыкновенные гомоморфизмы. Следовательно, мы немедленно заключаем coNP-полноту ограничения на связные графы задачи B-EVEN-HOM(Hex), а значит, и самой B-EVEN-HOM(Hex).

Литература

1. Bulatov A. A., Jeavons P., Krokhin A. A. The complexity of constraint satisfaction: An algebraic approach // Structural Theory of Automata, Semigroups, and Universal Algebra. Dordrecht, 2005. P. 131–170.
2. Bergman C., Slutzki G. Complexity of some problems concerning varieties and quasi-varieties of algebras // SIAM J. Comput. 2000. Vol. 30. P. 359–382.
3. Jackson M., McKenzie R. Interpreting graph colorability in finite semigroups // Int. J. Algebra and Computation. 2006. Vol. 16, № 1. P. 119–140.
4. Székely Z. Computational complexity of the finite algebra membership problem for varieties // Int. J. Algebra and Computation. 2002. Vol. 12, № 6. P. 811–823.
5. Kozik M. On some complexity problems in finite algebras: Dissertation / Vanderbilt University. Nashville, 2004.
6. Kharlampovich O., Sapir M. Algorithmic problems in varieties // Int. J. Algebra and Computation. 1995. Vol. 5. P. 379–602.
7. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
8. Papadimitriou C. H. Computational Complexity. New York: Addison-Wesley Publishing Company, 1994.
9. Burris S., Lawrence J. The equivalence problem for finite rings // Journal of Symbolic Computation. 1993. Vol. 15. P. 67–71.
10. Horváth G., Lawrence J., Mérai L., Szabó Cs. The complexity of the equivalence problem for nonsolvable groups. (Submitted).
11. Burris S., Lawrence J. Results on the equivalence problem for finite groups // Algebra Universalis. 2005. Vol. 52, № 4. P. 495–500.

12. Popov V. Yu., Volkov M. V. Complexity of checking identities and quasi-identities in finite semigroups. 2001. (Manuscript).

13. Kisielewicz A. Complexity of semigroup identity checking // Int. J. Algebra and Computation. 2004. Vol. 14, № 4. P. 455–464.

14. Szabó Cs., Vértesi V. The complexity of checking identities in $M_2(Z_2)$ // Proc. Amer. Math. Soc. 2004. Vol. 132. P. 3689–3695.

15. Klima O. Complexity issues of checking identities in finite monoids. (Manuscript).

16. Seif S. The Perkins semigroup has co-NP-complete term-equivalence problem // Int. J. Algebra and Computation. 2005. Vol. 15, № 2. P. 317–326.

17. Seif S., Szabó Cs. Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields // Semigroup Forum. 2006. Vol. 72. P. 207–222.

18. Feder T., Hell P., Huang J. List homomorphisms and circular arc graphs // Combinatorica. 1999. Vol. 19. P. 487–505.

19. Buki J., Szabó Cs. Colored homomorphisms for direct products of graphs // Information Processing Letters. 2002. Vol. 81, № 4. P. 175–178.

20. Клиффорд А., Престон Г. Алгебраическая теория полугрупп. М.: Мир, 1972. Т. 1.

21. Шеврин Л. Н., Волков М. В. Тождества полугрупп // Изв. вузов. Математика. 1989. № 11.

22. Машевицкий Г. И. О тождествах в многообразиях вполне простых полугрупп над абелевыми группами // Современ. алгебра. 1978. С. 81–89.

23. Rasin V. V. On the lattice of varieties of completely simple semigroups // Semigroup Forum. 1979. Vol. 17, № 2. P. 113–122.

24. Petrich M. Produit cartésien de demi-groupes complètement simples // C. R. Acad. Sci. (Paris). 1964. Vol. 259. P. 277–279.

25. Mashevitzky G. On the finite basis problem for completely 0-simple semigroup identities // Semigroup Forum. 1999. Vol. 59, № 2. P. 197–219.